

# [NT] Windows Address Book Contact Record Vulnerability (MS06-076)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-12/msg00017.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 13 Dec 2006 20:06:40 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Windows Address Book Contact Record Vulnerability (MS06-076)

---

## SUMMARY

A remote code execution vulnerability in a component of Outlook Express could allow an attacker who sent a Windows Address Book file to a user of an affected system to take complete control of the system.

## DETAILS

### Affected Software:

- \* Microsoft Windows 2000 Service Pack 4
- \* Microsoft Windows XP Service Pack 2
- \* Microsoft Windows XP Professional x64 Edition
- \* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- \* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- \* Microsoft Windows Server 2003 x64 Edition

### Non-Affected Software:

- \* Windows Vista

## [NT] Windows Address Book Contact Record Vulnerability (MS06-076)

### Affected Components:

\* Outlook Express 5.5 Service Pack 2 on Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=CB0563FB-A05D-4D9D-B269-B5602B09C16A>>  
Download the Update

\* Outlook Express 6 Service Pack 1 when installed on Microsoft Windows 2000 Service Pack 4 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1F0432D4-3F45-472E-8C2D-B7B6A879ACB8>>  
Download the update

\* Outlook Express 6 on Microsoft Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=560E8778-9733-4719-A565-614FD490C320>>  
Download the update

\* Outlook Express 6 on Microsoft Windows XP Professional x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?familyid=6BE4F4CE-ABD6-4A38-84A5-8952E3531217>>  
Download the update

\* Outlook Express 6 on Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=FE358108-15DF-4ED9-B257-01AEB82647DF>>  
Download the update

\* Outlook Express 6 on Microsoft Windows Server 2003 x64 Edition –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=DDE5C141-DE6C-4DD9-8399-6E5DB0DCC574>>  
Download the update

\* Outlook Express 6 on Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems –

<<http://www.microsoft.com/downloads/details.aspx?familyid=7D3FEA7A-DDC0-4A22-A8B3-D5F46707D017>>  
Download the update

Note: The security updates for Microsoft Windows Server 2003, Windows Server 2003 Service Pack 1, and Windows Server 2003 x64 Edition also apply to Windows Server 2003 R2.

Windows Address Book Contact Record Vulnerability – CVE-2006-2386:  
A remote code execution vulnerability in a component of Outlook Express could allow an attacker who sent a Windows Address Book file to a user of an affected system to take complete control of the system.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

Mitigating Factors for Windows Address Book Contact Record Vulnerability – CVE-2006-2386:

\* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

## [NT] Windows Address Book Contact Record Vulnerability (MS06–076)

\* In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to attempt to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site. In order for the exploit to take place, the user would have to open the .wab file.

\* In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted .wab file to the user and by persuading the user to open the file.

### Workarounds for Windows Address Book Contact Record Vulnerability – CVE–2006–2386:

Microsoft has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section:

\* Back up and remove the .wab file association

Removing the WAB registry key helps protect the affected system from attempts to exploit this vulnerability. To backup and remove the WAB registry key, follow these steps:

Warning: If you use Registry Editor incorrectly, you may cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that you can solve problems that result from using Registry Editor incorrectly. Use Registry Editor at your own risk.

We recommend backing up the registry before you edit it.

1. Click Start, click Run, type regedit" (without the quotation marks), and then click OK.
2. Expand HKEY\_CLASSES\_ROOT, and then click .WAB.
3. Click File, and then click Export.
4. In the Export Registry File dialog box, type a file name in the File Name box, and then click Save.
5. Click Edit, and then click Delete to remove the registry key.
6. In the Confirm Key Delete dialog box, you receive an Are you sure you want to delete this key and all of its subkeys message. Click Yes.

Impact of Workaround: Users will not be able to open address books by double clicking them. They will have to manually start the Windows Address Book application and pass the address book to be used as a command line parameter or they can import the address book from the File menu. This does not affect the use of address books in Outlook Express.

### FAQ for Windows Address Book Contact Record Vulnerability – CVE–2006–2386:

What is the scope of the vulnerability?

A remote code execution vulnerability in a component of Outlook Express could allow an attacker who sent a Windows Address Book file to a user of an affected system to take complete control of the system.

If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

What causes the vulnerability?

An unchecked buffer in the Windows Address Book (WAB) functions within Outlook Express.

What is a Windows Address Book?

Windows provides an address book for storing contact information. The WAB is an application and service that enables users to keep track of people. The WAB has a local database and user interface for finding and editing information about people.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system.

How could an attacker exploit the vulnerability?

In a Web-based attack scenario, an attacker would have to host a Web site that contains a Web page that is used to attempt to exploit this vulnerability. An attacker would have no way to force users to visit a malicious Web site. Instead, an attacker would have to persuade them to visit the Web site, typically by getting them to click a link that takes them to the attacker's site. In order for the exploit to take place, the user would have to open the .wab file.

In an e-mail attack scenario, an attacker could exploit the vulnerability by sending a specially-crafted .wab file to the user and by persuading the user to open the file.

A specially crafted .wab file opened from the local file system or from a network share could also allow lead to memory corruption that could potentially allow code execution.

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers could be at more risk if users who have sufficient administrative permissions are given the ability to log on to servers and to run programs. However, best practices strongly discourage allowing this.

What does the update do?

The update removes the vulnerability by modifying the way that Outlook Express, when using a .wab file, validates the length of a field before it passes it to the allocated buffer.

When this security bulletin was issued, had this vulnerability been

publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure. Microsoft had not received any information to indicate that this vulnerability had been publicly disclosed when this security bulletin was originally issued.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

ADDITIONAL INFORMATION

The original article can be found at:

<http://www.microsoft.com/technet/security/Bulletin/MS06-076.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS06-076.msp>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxx

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.